PCT/KR 03/00628
RO/KR 28.03.2003

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0071890
Application Number

출 원 년 월 일 : 2002년 11월 19일
Date of Application NOV 19, 2002

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

출 원 인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Institut

2003 년 02 월 25 일

특 허 청
COMMISSIONER

1020020071890

출력 일자: 2003/2/26

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0001
【제출일자】	2002.11.19
【발명의 명칭】	서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 방법 및 그 장치
【발명의 영문명칭】	METHOD AND APPARATUS FOR PROTECTING LEGITIMATE TRAFFIC FROM DoS AND DDoS ATTACKS
【출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
【대리인】	
【성명】	장성구
【대리인코드】	9-1998-000514-8
【포괄위임등록번호】	2001-038646-2
【대리인】	
【성명】	김원준
【대리인코드】	9-1998-000104-8
【포괄위임등록번호】	2001-038648-7
【발명자】	
【성명의 국문표기】	안개일
【성명의 영문표기】	AHN,Gaeil
【주민등록번호】	680101-1408715
【우편번호】	302-751
【주소】	대전광역시 서구 가수원동 은아아파트 102-106
【국적】	KR
【발명자】	
【성명의 국문표기】	김기영
【성명의 영문표기】	KIM,Ki Young
【주민등록번호】	660224-2551112

【우편번호】 305-755
【주소】 대전광역시 유성구 어은동 한빛아파트 122-601
【국적】 KR
【발명자】
【성명의 국문표기】 장종수
【성명의 영문표기】 JANG,Jong Soo
【주민등록번호】 611202-1670819
【우편번호】 305-761
【주소】 대전광역시 유성구 전민동 엑스포아파트 303-903
【국적】 KR

【공개형태】 학술단체 서면발표
【공개일자】 2002.10.15

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
장성구 (인) 대리인
김원준 (인)

【수수료】

【기본출원료】	20 면	29,000 원
【가산출원료】	10 면	10,000 원
【우선권주장료】	0 건	0 원
【심사청구료】	15 항	589,000 원
【합계】	628,000 원	
【감면사유】	정부출연연구기관	
【감면후 수수료】	314,000 원	

【기술이전】

【기술양도】	희망
【실시권 허여】	희망
【기술지도】	희망

【첨부서류】 1. 요약서·명세서(도면)_1통 2.공지예외적용대상(신규성상실의예외, 출원시의특례)규정을 적용받 기 위한 증명서류_1통

1020020071890

출력 일자: 2003/2/26

【요약서】

【요약】

본 발명은 악의 있는 사용자의 서비스 거부(Denial of Service, 이하 DoS라 칭함) 공격과 분산 서비스 거부(Distributed Denial of Service, 이하 DDoS라 칭함) 공격으로부터 발생되는 엄청난 양의 트래픽(traffic)으로부터 정상 사용자의 트래픽을 보호하는 방법 및 그 장치에 관한 것으로써 보호할 망 또는 인터넷 서버(internet server)의 앞단에 독자적으로 설치된다. 본 발명에서, 수신되는 모든 트래픽은 근원지 기반의 트래픽 트렁크(Source-based Traffic Trunk, 이하 STT라 칭함) 단위로 세분화되며, DDoS 트래픽(DoS 트래픽 포함)과 정상 트래픽을 차등 서비스할 목적으로 높은 순위의 큐와 낮은 순위의 큐를 사용한다. 본 발명에 따른 장치는 큐 정보 테이블을 유지하고 있는데, 이것은 각 STT에 대한 부하 정보와 서비스 큐 정보를 저장하고 있다. 패킷이 수신될 때마다 큐 정보 테이블에서 그 패킷에 해당되는 STT의 서비스 큐를 발견하여, 그 결과에 따라서 그 패킷은 높은 순위의 큐 또는 낮은 순위의 큐로 보내져 차등화된 서비스를 받는다. 즉, DoS와 DDoS 트래픽은 우선순위 낮은 큐를 사용하여 서비스되며, 정상 트래픽은 우선순위 높은 큐를 사용하여 서비스된다. 큐 정보 테이블에 저장된 각 STT들의 서비스 큐는 그 STT의 부하와 높은 우선 순위 큐의 부하에 따라서 동적으로 변경된다.

【대표도】

도 5

【명세서】

【발명의 명칭】

서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 방법 및 그 장치{METHOD AND APPARATUS FOR PROTECTING LEGITIMATE TRAFFIC FROM DoS AND DDoS ATTACKS}

【도면의 간단한 설명】

도 1은 종래 페어-큐잉의 기본 알고리즘을 나타낸 도면,

도 2는 종래 레이트-리미트의 기본 알고리즘을 나타낸 도면,

도 3은 전형적인 분산 서비스 거부 공격 모델링을 나타낸 도면,

도 4는 본 발명에서 제안하는 근원지 기반 트래픽 트렁크 개념을 적용했을 때의 분산 서비스 거부 공격 모델링을 나타낸 도면,

도 5는 본 발명에 따른 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 장치의 일 실시예를 나타낸 블록도,

도 6은 도 5에 도시된 패킷 분류기의 기본 알고리즘을 단계별로 나타낸 순서도,

도 7은 도 5에 도시된 큐 매핑기의 기본 알고리즘을 단계별로 나타낸 순서도,

도 8a는 도 7에 나타낸 큐 매핑기의 기본 알고리즘 중에서 패킷 정보 수신 단계와 수신된 패킷에 해당되는 근원지 기반의 트래픽 트렁크의 평균 부하 계산 단계에 대한 상세 알고리즘을 단계별로 나타낸 순서도,

도 8b는 도 7에 나타낸 큐 매핑기의 기본 알고리즘 중에서 근원지 기반의 트래픽 트렁크의 부하값에 기반하여 근원지 기반의 트래픽 트렁크 서비스 큐를 재 설정하는 단계에 대한 알고리즘을 단계별로 나타낸 순서도,

도 8c는 도 7에 나타낸 큐 매핑기의 기본 알고리즘 중에서 우선순위가 높은 큐의 평균 부하를 계산하는 단계의 알고리즘을 단계별로 나타낸 순서도,

도 8d는 도 7에 나타낸 큐 매핑기의 기본 알고리즘 중에서 우선순위 높은 큐의 부하값에 기반하여 근원지 기반의 트래픽 트렁크의 서비스 큐를 재 설정하는 단계의 알고리즘을 단계별로 나타낸 순서도,

도 9a는 서비스 거부와 분산 서비스 거부를 이용한 웹 서버 공격에서 종래의 페어-큐잉을 사용했을 때의 시뮬레이션 결과를 나타낸 도면,

도 9b는 서비스 거부와 분산 서비스 거부를 이용한 웹 서버 공격에서 본 발명에 따른 트래픽 제어 기술을 사용했을 때의 시뮬레이션 결과를 나타낸 도면.

<도면의 주요부분에 대한 부호의 설명>

501 : 정상 트래픽 보호 장치

502 : 큐 정보 테이블 503 : 큐 매핑기

504 : 패킷 분류기 505 : 우선순위 높은 큐

506 : 우선순위 낮은 큐 507 : 버퍼

508 : 망 접속 장치 509 : 망

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<20> 본 발명은 서비스 거부(Denial of Service, 이하 DoS라 칭함)와 분산 서비스 거부(Distributed Denial of Service, 이하 DDoS라 칭함) 공격으로부터 정상 트래픽(traffic)을 보호하는 방법 및 그 장치에 관한 것으로, 특히, DoS와 DDoS 공격에서 발생되는 엄청난 양의 트래픽으로부터 정상 트래픽을 보호하는 방법 및 그 장치에 관한 것이다.

<21> DoS 공격은 목적 망/서버에 단시간에 많은 트래픽을 집중시킴으로써 목적 시스템이 서비스를 제공할 수 없게 만드는 공격이다. DDoS 공격은 DoS 공격의 한 형태로써 수 많은 공격 사이트들이 한꺼번에 목적 망/서버에 트래픽을 집중시키는 공격으로써 DoS 공격보다 탐지 및 차단이 더 어려운 공격이다.

<22> 공격 방법에 따라서, DoS 공격은 TCP 프로토콜의 특성을 이용한 공격 유형과 단순히 트래픽을 폭주시키는 공격 유형으로 구분할 수 있다.

<23> 먼저, TCP 프로토콜의 특성을 이용한 공격 유형은 TCP 클라이언트가 TCP 서버와 연결을 설정할 때 3단계 오퍼레이션(즉, 첫번째로 클라이언트가 서버에게 SYN 패킷 보냄, 두 번째로 서버는 클라이언트에게 SYN-ACK 패킷 보냄, 마지막으로 클라이언트는 서버에게 ACK 패킷을 보냄)을 사용하는데, 이 특성을 이용한 공격으로써 TCP SYN 플러딩 공격이 있다. TCP SYN 플러딩 공격은 SYN 패킷을 계속 보내면서도 서버가 보낸 SYN-ACK 패킷을 무시하는 방법을 사용한 공격이다.

<24> 단순히 트래픽을 폭주시키는 방법을 사용하는 공격은 UDP 패킷 플러딩 공격, 핑(Ping) 요구 플러딩 공격, 그리고 HTTP 요구 플러딩 공격 등이 있다.

<25> 이러한 DoS 공격을 차단하기 위한 종래의 기술은 다음과 같다.

<26> (1) TCP 프로토콜의 서버 측 알고리즘을 개선하는 기술

<27> (2) 페어-큐잉(Fair-queuing) 기술

<28> (3) 레이트-리미트(Rate-limit) 기술

<29> TCP 프로토콜의 서버 측 알고리즘을 개선하는 기술은 기존 SYN 패킷 플러딩을 이용한 공격을 차단하는데 사용되는 제한적 기술로서 트래픽을 폭주시키는 공격은 막을 수 없는 기술이다.

<30> 페어-큐잉 기술은 라우터에서 폭주 제어와 공정한 자원(대역폭) 분배를 위하여 제안된 기술이다.

<31> 도 1은 종래 페어-큐잉의 기본 알고리즘을 나타낸 도면으로, 수신되는 패킷들은 각 플로우(flow) 별로 분리되어 해당 큐를 사용하여 다음 노드로 전송된다. 이때 큐들은 라운드 로빈(Round-robin) 방식으로 공평하게 서비스한다. 즉, 각 큐들은 총 링크 대역폭의 1/n 만큼씩 나누어 갖는다. 이 기술은 DoS 공격에서는 효과가 있지만, DDoS 공격에서는 효과적으로 그 공격을 차단할 수 없는 문제점을 가지고 있다. 즉, 악의있는 사용자가 플로우를 더 많이 생성하면 할수록 정상 사용자가 사용할 수 있는 대역폭은 그에 비례하여 더 줄어드는 문제가 있다.

<32> 레이트-리미트 기술은 TCP SYN 플러딩 공격 뿐만 아니라 트래픽 폭주 공격 들을 차단하기 위하여 제안된 기술이다.

<33> 도 2는 종래 레이트-리미트의 기본 알고리즘을 나타낸 도면으로, 레이트-리미트 기술은 특정 플로우들의 대역폭을 측정하여 그 값이 관리자가 정한 최대 허용 대역폭을 초과하면 그 초과분 패킷을 드랍(Drop)하는 기술이다. 이 기술은 두 가지 문제점을 가지고 있다. 첫 번째는 관리자가 최대 허용 대역폭을 정하기 위하여 일정 시간동안 망의 트래픽을 측정해야 하는 문제점이다. 두 번째는 DDoS 공격을 효과적으로 차단하기 어렵다는 것이다. DDoS 공격의 파괴력은 수 많은 공격 사이트들이 한 곳으로 집중하여 모아진 엄청난 트래픽 때문이다. 따라서 각각의 공격 사이트들이 발생 시키는 트래픽의 양은 그리 크지 않다. 즉, 공격 사이트와 정상 사이트에서 발생 시키는 트래픽의 차이가 크지 않는 DDoS 공격에서는 최대 허용 대역폭을 정하는 것이 매우 어려운 단점을 가지고 있다. 예를 들어 DDoS 트래픽을 차단하기 위하여 최대 허용 대역폭을 낮게 정하면 DDoS 트래픽 뿐만 아니라 정상 트래픽도 차단될 소지가 많은 문제점을 안고 있다.

<34> 위에서 설명한 바와 같이 종래의 기술들은 DoS 공격에서는 어느 정도의 효과가 있지만, DDoS 공격에서는 별 효과가 없으며, 또한 DDoS 공격을 차단할 수 있다고 해도 정상 트래픽을 보호하지 못하는 문제점을 안고 있다.

【발명이 이루고자 하는 기술적 과제】

<35> 본 발명은 상술한 결점을 해결하기 위하여 안출한 것으로, DoS 공격 뿐만 아니라 DDoS 공격으로부터 정상 사용자의 트래픽을 보호하는 방법 및 그 장치를 제공하는 데 그 목적이 있다.

<36> 이와 같은 목적을 달성하기 위한 본 발명은, 망 접속 장치와 보호할 망 사이에 접속되어 DoS와 DDoS 공격으로부터 정상 트래픽을 보호하는 장치에 있어서, 우선순위 높은 큐; 우선순위 낮은 큐; 특정 패킷이 속하는 특정 STT의 서비스 큐 정보를 저장하고 있

는 큐 정보 테이블; 제공되는 STT의 부하와 우선순위 높은 큐의 부하를 기반으로 상기 큐 정보 테이블을 갱신하는 큐 매핑기; 상기 망 접속 장치로부터 패킷을 수신하면 상기 큐 정보 테이블로부터 상기 수신된 패킷이 속하는 STT의 서비스 큐를 검색하여, 그 결과에 따라서 상기 우선순위 높은 큐 및 상기 우선순위 낮은 큐로 상기 수신된 패킷을 선택적으로 전달하고, 상기 수신된 패킷에 대한 정보를 상기 큐 매핑기로 제공하는 패킷 분류기; 및 상기 우선순위 높은 큐와 상기 우선순위 낮은 큐의 출력을 버퍼링하여 상기 보호할 망으로 제공하는 버퍼를 포함하는 것을 특징으로 한다.

【발명의 구성 및 작용】

<37> 이하, 첨부된 도면을 참조하여 본 발명에 따른 실시예를 상세히 설명하면 다음과 같다.

<38> DoS및 DDoS 트래픽을 플로우 단위로 처리하는 것은 성능, 부하, 공격 탐지의 정확도 측면에서 많은 단점이 있다. 본 발명에서는 근원지 기반의 트래픽 트렁크 (Source-based Traffic Trunk, 이하 STT라 칭함) 단위로 DoS와 DDoS 트래픽을 처리한다. 여기서, STT란 근원지의 네트워크 주소가 같은 플로우들의 집합을 말한다. 예로, 32bit IP 주소중 24bit로 STT를 만든다고 가정할 때, 168.188.44.0부터 168.188.44.255인 근원지 주소를 사용하는 모든 패킷은 168.188.44인 STT에 속하게 된다.

<39> 도 3은 전형적인 DDoS 공격 모델링을 나타낸 도면이고, 도 4는 본 발명에서 제안하는 STT 개념을 적용했을 때의 DDoS 공격 모델링을 나타낸 도면이다.

<40> DDoS 공격은 그 근원지가 전체 망에 고루 퍼져 있는 것이 아니라 보통 일부 망에 집중되어 있다. 예로, 해커가 전세계 모든 망에 있는 시스템을 골고루 해킹하여 DDoS 공

격 소프트웨어를 설치하는 것은 거의 불가능하며, 보통 일부 망만 해킹을 하고 있다. 또한 바이러스 예로, 님다 바이러스를 이용하여 불 특정 시스템에 침투하여 DDoS 공격을 실행하는 경우에서도 안전한 망 즉, 방화벽, 침입 탐지 시스템, 바이러스 치료 응용 등이 설치된 망에 침투하여 일정 시간 잠복하는 것은 매우 어려우며, 그래서 보통 안전하지 못한 망에서 잠복하고 있다. DDoS의 형태인 사이버 시위도 마찬가지로 보통 일부 집단 즉, 일부 망에서 수행되고 있다.

<41> 따라서 STT 방식은 플로우 방식보다 트래픽이 정상 트래픽인지 아닌지를 더 간단하면서도 더 정확하게 구분할 수 있다.

<42> 도 5는 본 발명에 따른 DoS와 DDoS 공격으로부터 정상 트래픽을 보호하는 장치의 일 실시예를 나타낸 블록도로, 정상 트래픽 보호 장치(501)는 망 접속 장치(508) 및 보호할 망(또는 보호할 서버)(509) 사이에 접속된다. 정상 트래픽 보호 장치(501)는 큐 정보 테이블(502), 큐 매핑기(503), 패킷 분류기(504), 우선순위 높은 큐(505), 우선순위 낮은 큐(506), 및 버퍼(507)로 구성된다.

<43> 동 도면에 있어서, 패킷 분류기(504)는 망 접속 장치(508)로부터 패킷을 수신하면 큐 정보 테이블(502)로부터 그 패킷이 속하는 STT의 서비스 큐를 검색하여, 그 결과에 따라서 우선순위 높은 큐(505) 또는 우선순위 낮은 큐(506)로 그 패킷을 전달한다. 그 패킷에 대한 정보 예로, 패킷 크기, 도착 시간, 및 그 패킷이 속하는 STT 정보를 가리키는 큐 정보 테이블(502)의 인덱스 등을 큐 매핑기(503)로 전달한다.

<44> 큐 매핑기(503)는 수신된 STT의 부하와 우선순위 높은 큐(505)의 부하를 기반으로 큐 정보 테이블(502)을 갱신하는 역할을 한다. 큐 정보 테이블(502)은 STT 식별자(STT

ID), 서비스 큐, 평균 부하, 최근의 부하계산한 시간, 및 수신된 총 패킷 크기를 최소한 포함하는 필드들로 구성되어 있다.

<45> 두 우선순위 높은 큐(505)와 우선순위 낮은 큐(506)가 견딜 수 있는 최대 부하는 보호할 망(509) 또는 서버가 허용할 수 있는 최대 부하로 설정한다. 예로, 보호할 시스템이 허용할 수 있는 최대 부하가 100이라면 두 우선순위 높은 큐(505)와 우선순위 낮은 큐(506)가 견딜 수 있는 총 부하의 합은 100으로 설정되어야 한다. 우선순위 높은 큐(505)와 우선순위 낮은 큐(506) 모두에 패킷이 있다면, 우선순위 높은 큐(505)에 있는 패킷이 먼저 서비스된다.

<46> 버퍼(507)는 우선순위 높은 큐(505)와 우선순위 낮은 큐(506)의 출력을 버퍼링하여 보호할 망(509)으로 제공한다.

<47> 도 6은 도 5에 도시된 패킷 분류기(504)의 기본 알고리즘을 단계별로 나타낸 순서도이다.

<48> 먼저, 패킷 분류기(504)는 망 접속 장치(508)로부터 패킷을 수신한다(단계 601). 패킷 분류기(504)는 수신한 패킷의 근원지 IP 주소를 가지고 STT 식별자를 알아낸다(단계 602). 패킷 분류기(504)는 큐 정보 테이블(502)로부터 알아낸 STT 식별자에 해당되는 서비스 큐를 검색한다(단계 603). 패킷 분류기(504)는 검색 결과 값에 따라서 우선순위 높은 큐(505) 및 우선순위 낮은 큐(506)에 수신한 패킷을 선택적으로 전달한다(단계 604, 605, 606). 패킷 분류기(504)는 큐 매핑기(503)로 패킷 정보를 전달한다(단계 607).

<49> 도 7은 도 5에 도시된 큐 매핑기(503)의 기본 알고리즘을 단계별로 나타낸 순서도이다.

<50> 먼저, 큐 매핑기(503)는 패킷 분류기(504)로부터 패킷 정보를 수신한다(단계 702). 큐 매핑기(503)는 수신한 패킷에 해당되는 STT의 평균 부하를 계산한다(단계 703). 큐 매핑기(503)는 계산한 STT의 평균 부하 값에 기반하여 STT의 서비스 큐를 재 설정한다(단계 704). 큐 매핑기(503)는 우선순위 높은 큐(505)의 평균 부하를 계산한다(단계 705). 큐 매핑기(503)는 계산한 우선순위 높은 큐(505)의 평균 부하 값에 기반하여 일부 STT의 서비스 큐를 재 설정한다(단계 706). 큐 매핑기(503)는 변경된 평균 부하 값과 서비스 큐 등의 변경된 STT 정보를 큐 정보 테이블(502)에 저장한다(단계 707).

<51> 도 8a는 도 7에 나타낸 큐 매핑기(503)의 기본 알고리즘 중에서 패킷 정보 수신 단계(702)와 수신된 패킷에 해당되는 STT의 평균 부하 계산 단계(703)에 대한 상세 알고리즘을 단계별로 나타낸 순서도이다.

<52> 먼저, 큐 매핑기(503)는 패킷 분류기(504)로부터 패킷 크기, 도착 시간, 큐 정보 테이블 인덱스, 해당 STT 등의 패킷 정보를 수신한다(단계 802). 큐 매핑기(503)는 수신된 패킷 정보로부터 수신된 총 패킷 크기를 계산한다(단계 803). 이때, "총 패킷 크기 = 총 패킷 크기 + 수신된 패킷의 크기"이다. 큐 매핑기(503)는 평균 부하를 재 계산할 시간인지 여부를 판단한다(단계 804). 큐 매핑기(503)는 단계 804의 판단 결과, 평균 부하를 재 계산할 시간이면 이전 평균 부하값과 총 패킷 크기에 기반한 현재 평균 부하값을 고려하여 새로운 평균 부하값을 계산한다(단계 805). 이때, "평균 부하값 = (이전 평균 부하값 * α + 총 패킷 크기)/((패킷 도착 시간 - 최근 부하 계산 시간) * (1-α)), 단 $0<\alpha<1$)"이다. 여기서, 부하를 계산하는 시간 주기는 사용자에 의해서 미리 정해진다.

큐 매핑기(503)는 단계 804의 판단 결과, 평균 부하를 재 계산할 시간이 아니거나 단계 805를 수행한 후 STT의 부하값에 의한 STT 서비스 큐 결정 알고리즘을 수행한다(단계 806).

<53> 도 8b는 도 7에 나타낸 큐 매핑기(503)의 기본 알고리즘 중에서 STT의 부하값에 기반하여 STT 서비스 큐를 재 설정하는 단계(704)에 대한 알고리즘을 단계별로 나타낸 순서도이다. 도 8b는 패킷이 도착할 때마다 실행되는 알고리즘으로써 그 목적은 평균 부하값이 상대적으로 높은 STT는 우선순위 낮은 큐(506)를 사용하게 만드는 것이며, 반대로 평균 부하값이 상대적으로 낮은 STT는 우선순위 높은 큐(505)를 사용하게 만드는 것이다. 즉, DoS 및 DDoS 트래픽들이 우선순위 낮은 큐를 사용하게 만드는 것이다.

<54> 먼저, 큐 매핑기(503)는 우선 순위 높은 큐(505)가 폭주 상태인지 여부를 판단한다(단계 808). 큐 매핑기(503)는 단계 808의 판단 결과, 우선 순위 높은 큐(505)가 폭주 상태일 경우 수신된 패킷의 STT 부하가 허용 부하 보다 큰지 여부를 판단한다(단계 809). 큐 매핑기(503)는 단계 809의 판단 결과, 수신된 패킷의 STT 부하가 허용 부하 보다 크면 수신된 패킷의 STT의 서비스 큐를 우선순위 낮은 큐(506)로 설정한다(단계 810). 여기서, 허용 부하는 "우선순위 높은 큐(505)의 평

균부하 / 부하 재 계산 시간 간격동안 우선순위 높은 큐(505)를 사용한 STT의 수"이다. 이 알고리즘에 의하여 DDoS 트래픽일 가능성이 있는 STT들은 우선순위 낮은 큐(506)로 재빠르게 몰리게 된다. 큐 매핑기(503)는 수신된 패킷에 해당하는 STT의 서비스 큐가 우선순위 높은 큐인지 우선 순위 낮은 큐인지를 판단한다(단계 811). 큐 매핑기(503)는 단계 811의 판단 결과, 수신된 패킷에 해당하는 STT의 서비스 큐가 우선순위 높은 큐이면 큐 정보 테이블(502)에서 우선 순위 낮은 큐를 사용하는 STT 하나를 임으로 선택한다(단계 812). 큐 매핑기(503)는 수신된 패킷에 해당하는 STT의 평균 부하와 임의로 선택된 STT의 평균 부하를 비교한다(단계 813). 큐 매핑기(503)는 단계 813의 비교 결과, 수신된 패킷에 해당하는 STT의 평균 부하가 임의로 선택된 STT의 평균 부하보다 클 경우 부하가 낮은 STT는 그 서비스 큐를 우선순위 높은 큐로 설정하고 부하가 높은 STT는 그 서비스 큐를 우선순위 낮은 큐로 설정한다(단계 814). 큐 매핑기(503)는 단계 811의 판단 결과, 수신된 패킷에 해당하는 STT의 서비스 큐가 우선순위 낮은 큐일 경우에는 큐 정보 테이블(502)에서 우선 순위 높은 큐를 사용하는 STT 하나를 임으로 선택한다(단계 815). 큐 매핑기(503)는 수신된 패킷에 해당하는 STT의 평균 부하와 임의로 선택된 STT의 평균 부하를 비교한다(단계 816). 큐 매핑기(503)는 단계 816의 비교 결과, 수신된 패킷에 해당하는 STT의 평균 부하가 임의로 선택된 STT의 평균 부하보다 작을 경우 부하가 낮은 STT는 그 서비스 큐를 우선순위 높은 큐로 설정하고 부하가 높은 STT는 그 서비스 큐를 우선순위 낮은 큐로 설정한다(단계 817). 이 알고리즘에 의해서 정상 트래픽은 우선순위 높은 큐를 사용하게 되고, DDoS 트래픽은 우선순위 낮은 큐를 사용하게 된다.

<55> 도 8c는 도 7에 나타낸 큐 매핑기(503)의 기본 알고리즘 중에서 우선순위 높은 큐(505)의 평균 부하를 계산하는 단계(705)의 알고리즘을 단계별로 나타낸 순서도이다. 이 알고리즘은 수신된 패킷의 서비스 큐가 우선순위 높은 큐일 때만 실행된다.

<56> 먼저, 큐 매핑기(503)는 STT의 부하값에 의한 STT 서비스 큐를 결정한다(단계 819). 큐 매핑기(503)는 수신된 패킷이 사용한 서비스 큐가 우선순위 높은 큐인지 우선순위 낮은 큐인지를 판단한다(단계 820). 큐 매핑기(503)는 단계 820의 판단 결과, 수신된 패킷이 사용한 서비스 큐가 우선순위 높은 큐일 경우 우선순위 높은 큐로 서비스하는 총 패킷 크기를 계산한다(단계 821). 큐 매핑기(503)는 부하 재 계산할 시간인지 여부를 판단한다(단계 822). 큐 매핑기(503)는 단계 822의 판단 결과, 부하 재 계산할 시간이면 우선순위 높은 큐의 평균 부하를 계산한다(단계 823). 큐 매핑기(503)는 우선순위 높은 큐의 부하값에 의한 일부 STT의 서비스 큐를 재 설정한다(단계 824). 큐 매핑기(503)는 변경된 STT 정보를 큐 정보 테이블(502)에 저장한다(단계 825).

<57> 도 8d는 도 7에 나타낸 큐 매핑기(503)의 기본 알고리즘 중에서 우선순위 높은 큐의 부하값에 기반하여 STT의 서비스 큐를 재 설정하는 단계(706)의 알고리즘을 단계별로 나타낸 순서도이다. 이 알고리즘은 우선순위 높은 큐의 평균 부하가 계산될 때 마다 실행된다.

<58> 먼저, 큐 매핑기(503)는 우선순위 높은 큐의 평균 부하를 계산한다(단계 826). 큐 매핑기(503)는 우선순위 높은 큐의 부하가 폭주 상태, 한가 상태, 및 안정 상태 중 어느 상태인지를 판단한다(단계 827). 큐 매핑기(503)는 단계 827의 판단 결과, 우선순위 높은 큐의 부하가 폭주 상태일 경우에는 우선순위 높은 큐를 사용하는 STT들 중 임으로 하나를 선택하여 그 STT가 우선순위 낮은 큐를 사용하도록 설정한다(단계 828, 829).

반면, 큐 매핑기(503)는 단계 827의 판단 결과, 우선순위 높은 큐의 부하가 한가 상태일 때는 그 우선순위 낮은 큐를 사용하는 STT들 중 임으로 하나를 선택하여 그 STT가 우선순위 높은 큐를 사용하도록 설정한다(단계 830, 831). 큐 매핑기(503)는 단계 827의 판단 결과, 우선순위 높은 큐의 부하가 안정 상태이거나 단계 829, 831을 수행한 후에는 변경된 STT 정보를 큐 정보 테이블(502)에 저장한다(단계 832). 이 알고리즘에 의하여 우선 순위 높은 큐는 일정한 부하를 유지할 수 있으며, 따라서 우선 순위 높은 큐를 사용하는 STT들 즉, 정상 트래픽은 좋은 서비스 품질을 보장받을 수 있다.

<59> 도 9a는 DoS와 DDoS를 이용한 웹 서버 공격에서 종래의 페어-큐잉을 사용했을 때의 시뮬레이션 결과를 나타낸 도면이고, 도 9b는 DoS와 DDoS를 이용한 웹 서버 공격에서 본 발명에 따른 트래픽 제어 기술을 사용했을 때의 시뮬레이션 결과를 나타낸 도면이다.

<60> 종래에는 정상 트래픽이 도 9a와 같이 두 DoS와 DDoS 공격에 ??은 영향을 받지만, 본 발명을 적용시켰을 때는 정상 트래픽이 도 9b와 같이 두 DoS와 DDoS 공격에 거의 영향을 받지 않는다.

【발명의 효과】

<61> 이상에서 설명한 바와 같이, 본 발명은 STT 단위로 트래픽을 구분하기 때문에, 플로우 방식보다 장치의 성능에 큰 영향을 주지 않으면서도 더 정확하게 부하를 측정할 수 있다. 특정 STT가 DDoS 트래픽인지 정상 트래픽인지의 판단은 그 STT에 속하는 패킷이 수신될 때마다 행해지기 때문에, DDoS 트래픽은 도 8b와 같이 매우 빠르게 우선순위 낮은 큐로 설정된다. DDoS 공격으로 트래픽이 급격히 증가하더라도 정상 트래픽이 사용하는 우선순위 높은 큐의 부하를 일정하게 유지시키기 때문에, 정상 트래픽의 소실을 도

8b 및 도 8d와 같이 최소화 시킬 수 있다. 특정 시스템이 많은 트래픽을 생성하더라도 망 자원에 여유가 있다면, 그 트래픽은 차단되지 않는다.

【특허청구범위】

【청구항 1】

망 접속 장치와 보호할 망 사이에 접속되어 DoS와 DDoS 공격으로부터 정상 트래픽을 보호하는 장치에 있어서,

우선순위 높은 큐;

우선순위 낮은 큐;

특정 패킷이 속하는 특정 STT의 서비스 큐 정보를 저장하고 있는 큐 정보 테이블;

제공되는 STT의 부하와 우선순위 높은 큐의 부하를 기반으로 상기 큐 정보 테이블을 갱신하는 큐 매핑기;

상기 망 접속 장치로부터 패킷을 수신하면 상기 큐 정보 테이블로부터 상기 수신된 패킷이 속하는 STT의 서비스 큐를 검색하여, 그 결과에 따라서 상기 우선순위 높은 큐 및 상기 우선순위 낮은 큐로 상기 수신된 패킷을 선택적으로 전달하고, 상기 수신된 패킷에 대한 정보를 상기 큐 매핑기로 제공하는 패킷 분류기; 및

상기 우선순위 높은 큐와 상기 우선순위 낮은 큐의 출력을 버퍼링하여 상기 보호할 망으로 제공하는 버퍼를 포함하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 장치.

【청구항 2】

제 1 항에 있어서, 상기 보호할 망은 서버로 구성되는 것을 특징으로 하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 장치.

【청구항 3】

제 1 항에 있어서, 상기 수신된 패킷에 대한 정보는 패킷 크기, 도착 시간, 및 그 패킷이 속하는 STT 정보를 가리키는 상기 큐 정보 테이블의 인덱스를 포함하는 것을 특징으로 하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 장치.

【청구항 4】

제 1 항에 있어서, 상기 큐 정보 테이블은 STT 식별자, 서비스 큐, 평균 부하, 최근의 부하계산한 시간, 및 수신된 총 패킷 크기를 최소한 포함하는 필드들로 구성되어 있는 것을 특징으로 하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 장치.

【청구항 5】

제 1 항에 있어서, 상기 우선순위 높은 큐와 상기 우선순위 낮은 큐가 견딜 수 있는 최대 부하는 상기 보호할 망이 허용할 수 있는 최대 부하로 설정되는 것을 특징으로 하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 장치.

【청구항 6】

제 5 항에 있어서, 상기 보호할 망은 서버로 구성되는 것을 특징으로 하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 장치.

【청구항 7】

특정 패킷이 속하는 특정 STT의 서비스 큐 정보를 저장하고 있는 큐 정보 테이블, 제공되는 STT의 부하와 기설정된 우선순위 높은 큐의 부하를 기반으로 상기 큐 정보 테

이블을 갱신하는 큐 매핑기, 및 기설정된 망 접속 장치로부터 패킷을 수신하면 상기 큐 정보 테이블로부터 상기 수신된 패킷이 속하는 STT의 서비스 큐를 검색하여 그 결과에 따라서 상기 우선순위 높은 큐 및 기설정된 우선순위 낮은 큐로 상기 수신된 패킷을 선택적으로 전달하고 상기 수신된 패킷에 대한 정보를 상기 큐 매핑기로 제공하는 패킷 분류기를 포함하고 망 접속 장치와 보호할 망 사이에 접속되어, DoS와 DDoS 공격으로부터 정상 트래픽을 보호하는 장치에서 정상 트래픽을 보호하는 방법에 있어서,

상기 패킷 분류기는 상기 망 접속 장치로부터 수신한 패킷의 근원지 IP 주소를 가지고 STT 식별자를 알아내는 제 1 단계;

상기 큐 정보 테이블을 검색해서 상기 알아낸 STT 식별자에 해당되는 서비스 큐를 검색하여 높은 우선 순위 큐인지 낮은 우선 순위 큐인지를 판단하는 제 2 단계;

상기 제 2 단계의 판단 결과, 높은 우선 순위 큐이면 상기 수신한 패킷을 상기 우선순위 높은 큐로 전달하는 제 3 단계;

상기 제 2 단계의 판단 결과, 낮은 우선 순위 큐이면 상기 수신한 패킷을 상기 우선순위 낮은 큐로 전달하는 제 4 단계; 및

상기 수신한 패킷 정보를 상기 큐 매핑기로 전달하는 제 5 단계를 수행하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 방법.

【청구항 8】

제 7 항에 있어서, 상기 보호할 망은 서버로 구성되는 것을 특징으로 하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 방법.

【청구항 9】

제 7 항에 있어서,

상기 큐 매핑기는 상기 패킷 분류기로부터 전달받은 패킷 정보에 해당되는 STT의 평균 부하를 계산하는 제 71 단계;

상기 계산한 STT의 평균 부하 값에 기반하여 STT의 서비스 큐를 재 설정하는 제 72 단계;

상기 우선순위 높은 큐의 평균 부하를 계산하는 제 73 단계;

상기 계산한 우선순위 높은 큐의 평균 부하 값에 기반하여 일부 STT의 서비스 큐를 재 설정하는 제 74 단계; 및

상기 재 설정된 STT 정보를 상기 큐 정보 테이블에 저장하는 제 75 단계를 수행하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 방법.

【청구항 10】

제 9 항에 있어서, 상기 변경된 STT 정보는 변경된 평균 부하 값과 서비스 큐인 것을 특징으로 하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 방법.

【청구항 11】

제 9 항에 있어서,

상기 제 71 단계는 상기 패킷 분류기로부터 전달받은 패킷 정보로부터 수신된 총 패킷 크기를 계산하는 제 91 단계;

평균 부하를 재 계산할 시간인지 여부를 판단하는 제 92 단계;

상기 제 92 단계의 판단 결과, 평균 부하를 재 계산할 시간이면 이전 평균 부하값과 상기 총 패킷 크기에 기반한 현재 평균 부하값을 고려하여 새로운 평균 부하값을 계산하는 제 93 단계; 및

상기 제 92 단계의 판단 결과, 평균 부하를 재 계산할 시간이 아니거나 상기 제 93 단계를 수행한 후 STT의 부하값에 의한 STT 서비스 큐 결정 알고리즘을 수행하는 제 94 단계를 포함하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 방법.

【청구항 12】

제 11 항에 있어서, 상기 패킷 정보는 패킷 크기, 도착 시간, 큐 정보 테이블 인덱스, 해당 STT를 포함하는 것을 특징으로 하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 방법.

【청구항 13】

제 9 항에 있어서,

상기 제 72 단계는 상기 우선 순위 높은 큐가 폭주 상태일 경우 수신된 패킷의 STT 부하가 허용 부하 보다 크면 수신된 패킷의 STT의 서비스 큐를 상기 우선순위 낮은 큐로 설정하는 제 810 단계;

수신된 패킷에 해당하는 STT의 서비스 큐가 우선순위 높은 큐이면 상기 큐 정보 테이블에서 우선 순위 낮은 큐를 사용하는 STT 하나를 임으로 선택하는 제 811 단계;

수신된 패킷에 해당하는 STT의 평균 부하가 상기 임의로 선택된 STT의 평균 부하보다 클 경우 부하가 낮은 STT는 그 서비스 큐를 우선순위 높은 큐로 설정하고 부하가 높은 STT는 그 서비스 큐를 우선순위 낮은 큐로 설정하는 제 812 단계;

수신된 패킷에 해당하는 STT의 서비스 큐가 우선순위 낮은 큐일 경우에는 상기 큐 정보 테이블에서 우선 순위 높은 큐를 사용하는 STT 하나를 임으로 선택하는 제 813 단계; 및

수신된 패킷에 해당하는 STT의 평균 부하가 상기 임의로 선택된 STT의 평균 부하보다 작을 경우 부하가 낮은 STT는 그 서비스 큐를 우선순위 높은 큐로 설정하고 부하가 높은 STT는 그 서비스 큐를 우선순위 낮은 큐로 설정하는 제 814 단계를 포함하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 방법.

【청구항 14】

제 9 항에 있어서,

상기 제 73 단계는 STT의 부하값에 의한 STT 서비스 큐를 결정하는 제 821 단계;

수신된 패킷이 사용한 서비스 큐가 우선순위 높은 큐일 경우 우선순위 높은 큐로 서비스하는 총 패킷 크기를 계산하는 제 822 단계;

부하 재 계산할 시간이면 우선순위 높은 큐의 평균 부하를 계산하는 제 823 단계;

우선순위 높은 큐의 부하값에 의한 일부 STT의 서비스 큐를 재 설정하는 제 824 단계; 및

변경된 STT 정보를 상기 큐 정보 테이블에 저장하는 제 825 단계를 포함하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 방법.

【청구항 15】

제 9 항에 있어서,

상기 제 74 단계는 우선순위 높은 큐의 평균 부하를 계산하는 제 826 단계;

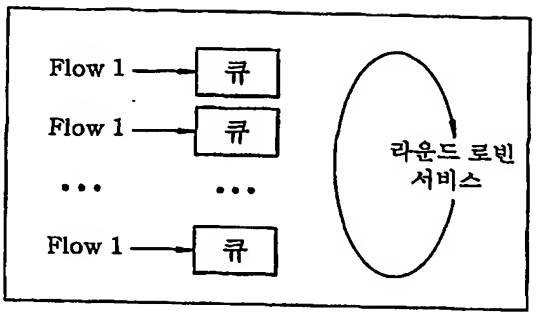
우선순위 높은 큐의 부하가 폭주 상태일 경우에는 우선순위 높은 큐를 사용하는 STT들 중 임으로 하나를 선택하여 그 STT가 우선순위 낮은 큐를 사용하도록 설정하는 제 827 단계;

우선순위 높은 큐의 부하가 한가 상태일때는 그 우선순위 낮은 큐를 사용하는 STT들 중 임으로 하나를 선택하여 그 STT가 우선순위 높은 큐를 사용하도록 설정하는 제 828 단계; 및

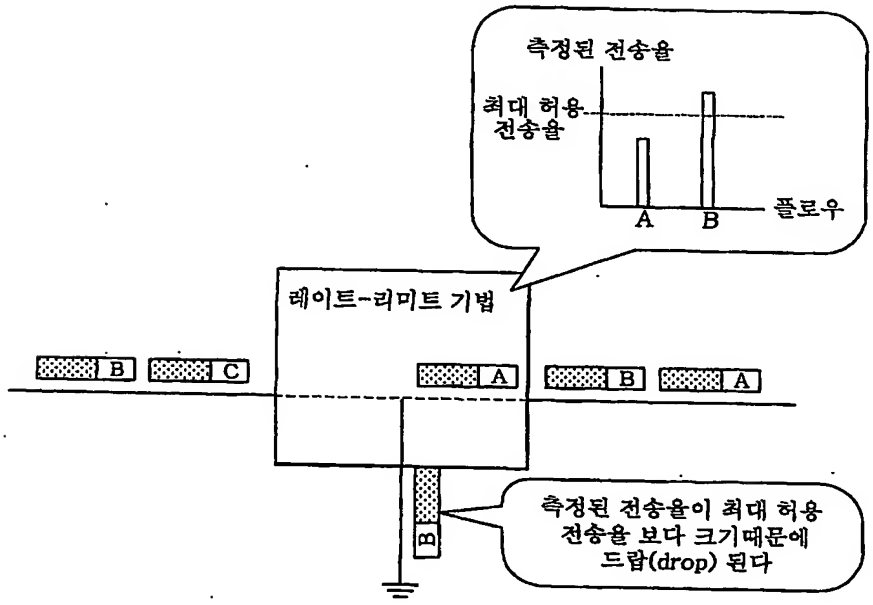
우선순위 높은 큐의 부하가 안정 상태이거나 제 827, 828 단계를 수행한 후에는 변경된 STT 정보를 상기 큐 정보 테이블에 저장하는 제 829 단계를 포함하는 서비스 거부와 분산 서비스 거부 공격으로부터 정상 트래픽을 보호하는 방법.

【도면】

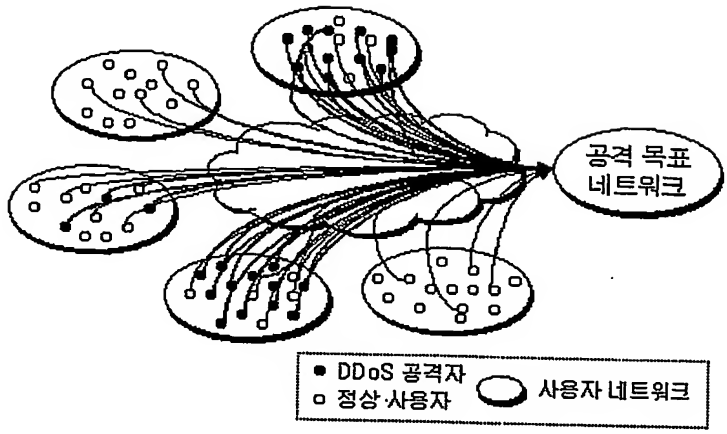
【도 1】


Flow 1
큐
Flow 1
큐
Flow 1
큐
라운드 로빈
서비스

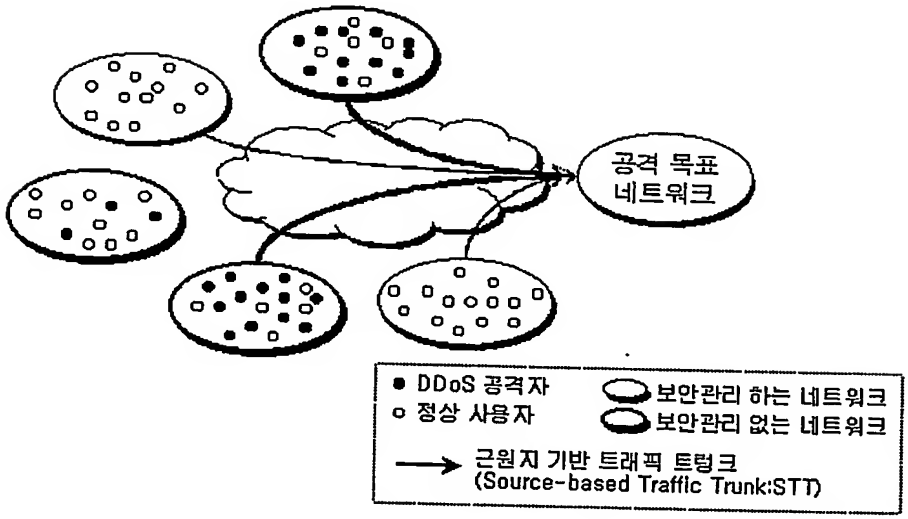
【도 2】


측정된 전송율
최대 허용
전송율
A
B
플로우
레이트-리미트 기법
B
C
A
B
A
B
측정된 전송율이 최대 허용
전송율 보다 크기때문에
드랍(drop) 된다

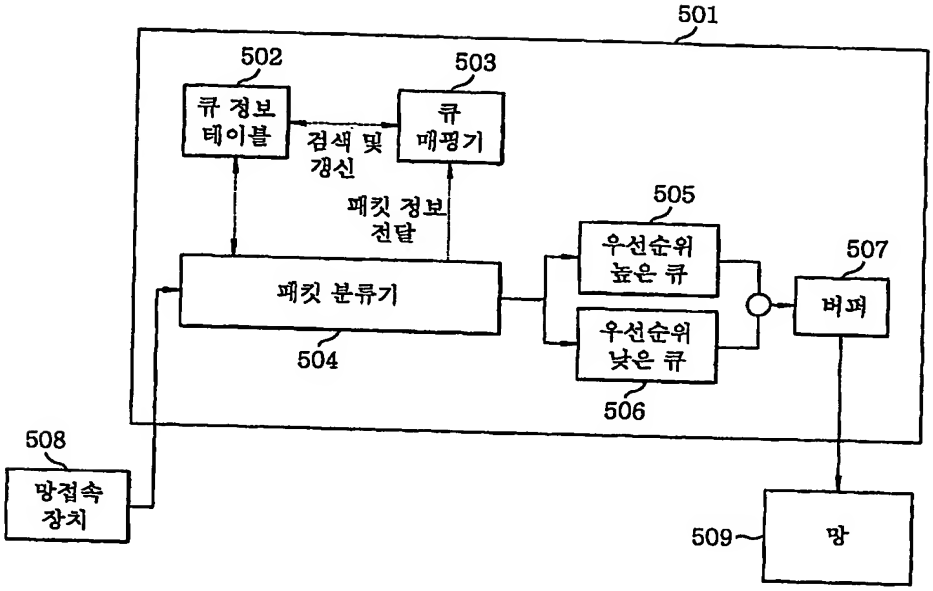
【도 3】


공격 목표
네트워크
DDoS 공격자
정상 사용자
사용자 네트워크

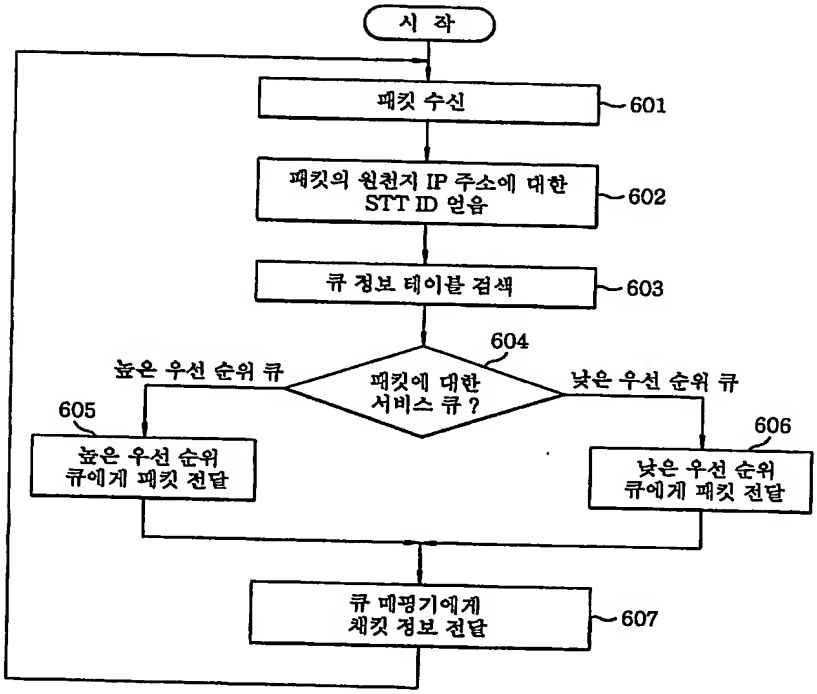
【도 4】


공격 목표
네트워크
DDoS 공격자
정상 사용자
보안관리 하는 네트워크
보안관리 없는 네트워크
근원지 기반 트래픽 트렁크
(Source-based Traffic Trunk:STT)

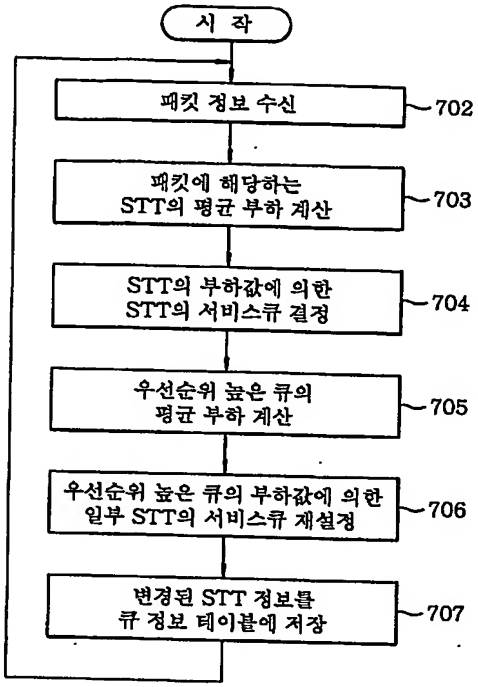
【도 5】


501
502
큐 정보 테이블
503
큐 매핑기
검색 및 갱신
패킷 정보 전달
505
우선순위 높은 큐
507
버퍼
패킷 분류기
504
우선순위 낮은 큐
506
508
망접속 장치
509
망

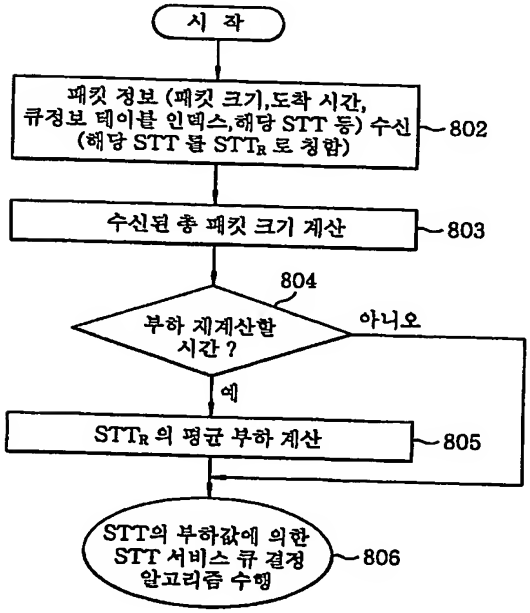
【도 6】


시 작
패킷 수신
601
패킷의 원천지 IP 주소에 대한 STT ID 얻음
602
큐 정보 테이블 검색
603
604
높은 우선 순위 큐
패킷에 대한 서비스 큐 ?
낮은 우선 순위 큐
605
높은 우선 순위 큐에게 패킷 전달
606
낮은 우선 순위 큐에게 패킷 전달
큐 매핑기에게 패킷 정보 전달
607

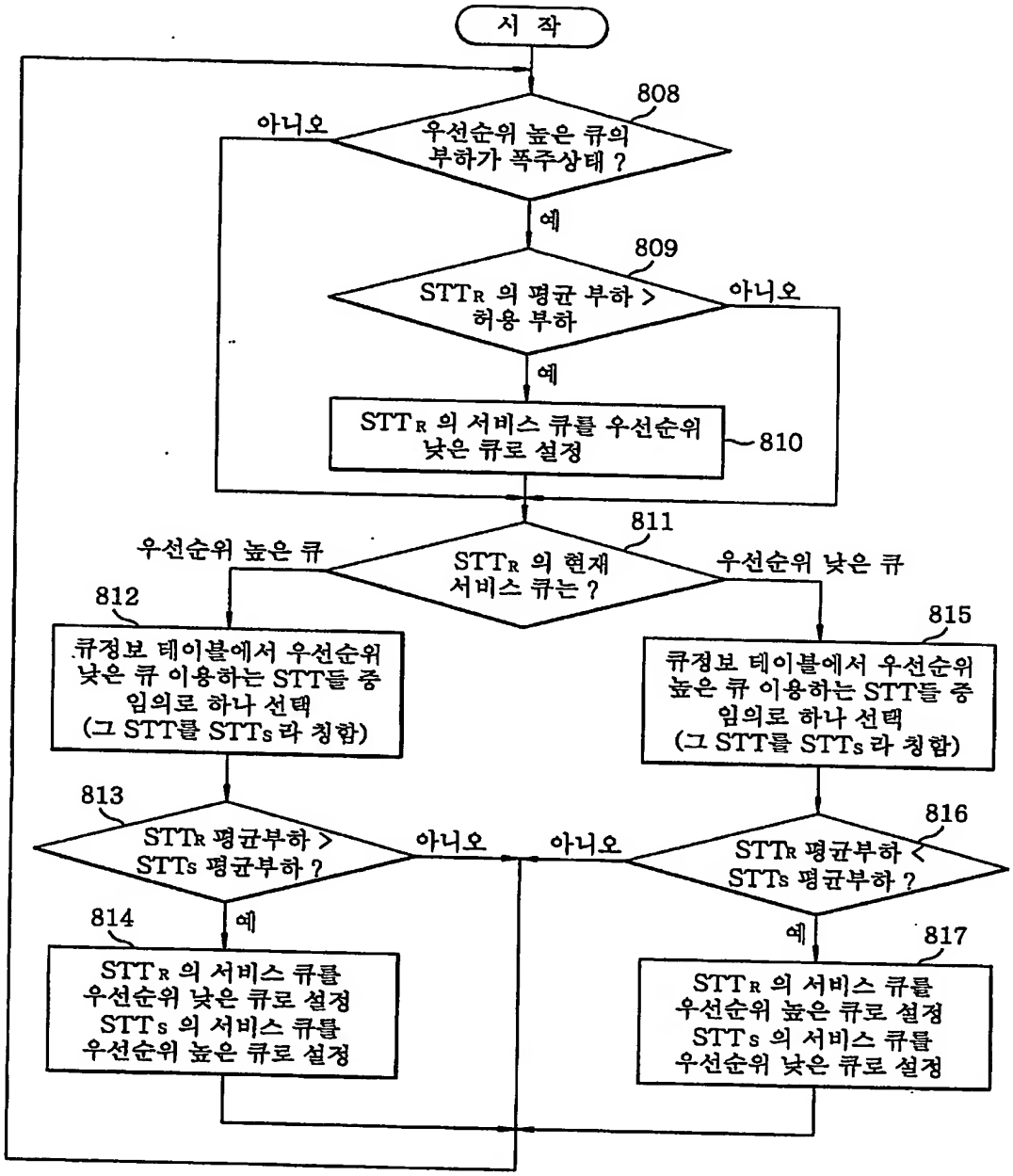
【도 7】


시 작
패킷 정보 수신
702
패킷에 해당하는 STT의 평균 부하 계산
703
STT의 부하값에 의한 STT의 서비스큐 결정
704
우선순위 높은 큐의 평균 부하 계산
705
우선순위 높은 큐의 부하값에 의한 일부 STT의 서비스큐 재설정
706
변경된 STT 정보를 큐 정보 테이블에 저장
707

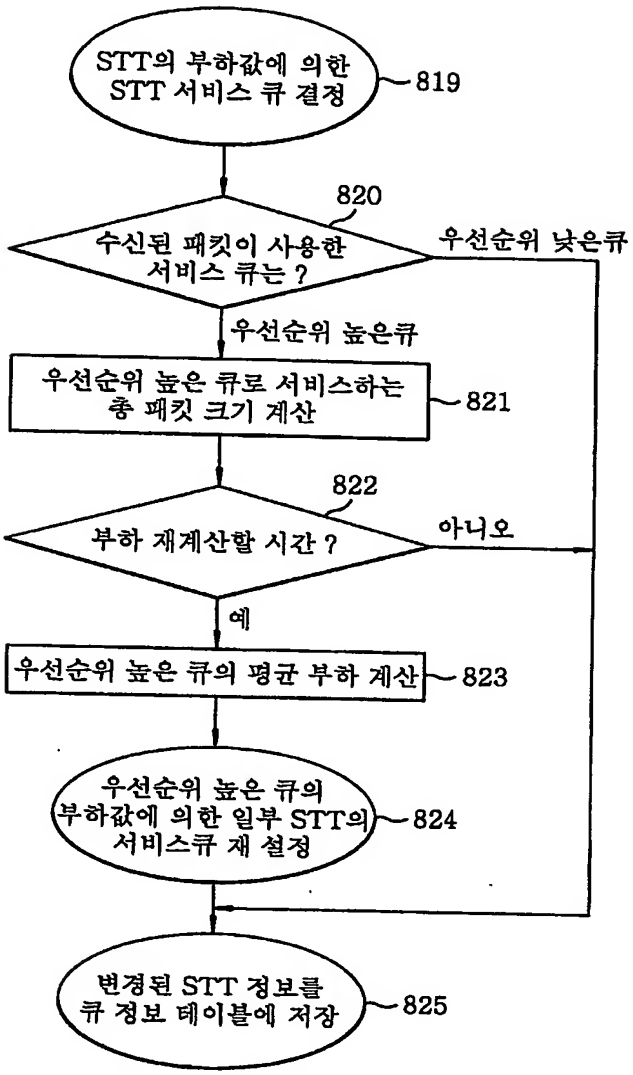
【도 8a】


시 작
패킷 정보 (패킷 크기,도착 시간, 큐정보 테이블 인덱스,해당 STT 등) 수신 (해당 STT 를 STT_R 로 칭함)
802
수신된 총 패킷 크기 계산
803
804
부하 재계산할 시간 ?
아니오
예
STT_R 의 평균 부하 계산
805
STT의 부하값에 의한 STT 서비스 큐 결정 알고리즘 수행
806

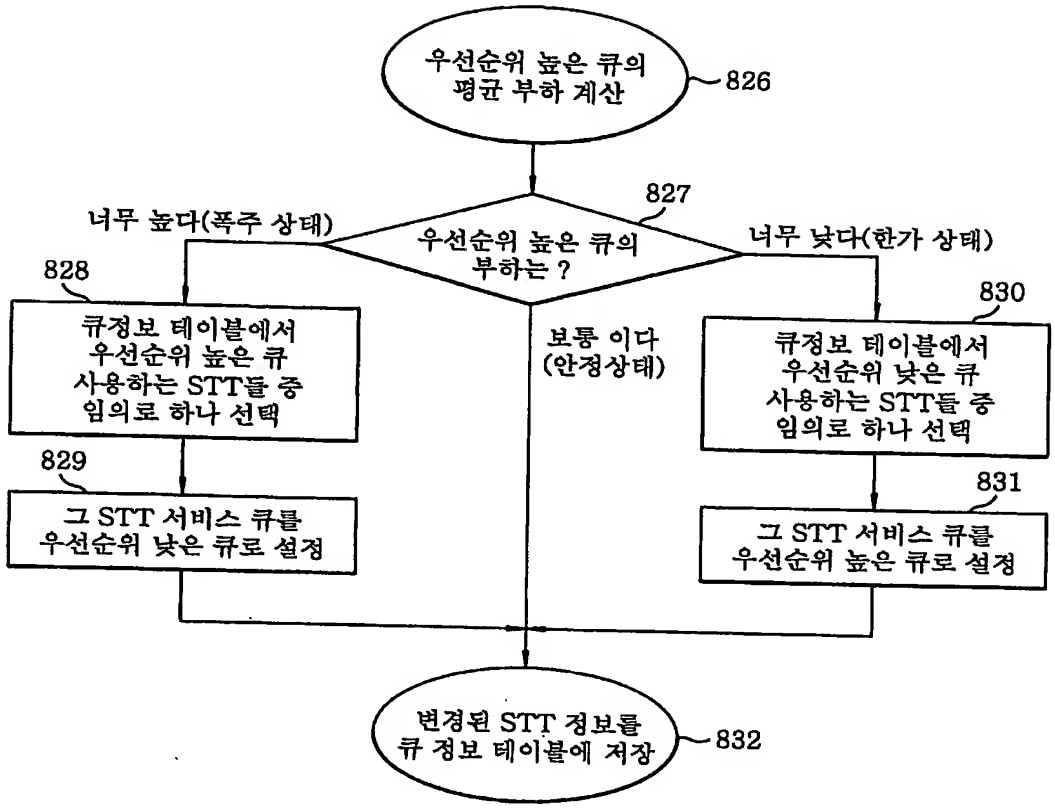
【도 8b】


시 작
808
우선순위 높은 큐의 부하가 폭주상태 ?
아니오
예
809
STTR 의 평균 부하 > 허용 부하
아니오
예
STTR 의 서비스 큐를 우선순위 낮은 큐로 설정
810
811
STTR 의 현재 서비스 큐는 ?
우선순위 높은 큐
우선순위 낮은 큐
812
큐정보 테이블에서 우선순위 낮은 큐 이용하는 STT들 중 임의로 하나 선택 (그 STT를 STTS 라 칭함)
815
큐정보 테이블에서 우선순위 높은 큐 이용하는 STT들 중 임의로 하나 선택 (그 STT를 STTS 라 칭함)
813
STTR 평균부하 > STTS 평균부하 ?
아니오
아니오
816
STTR 평균부하 < STTS 평균부하 ?
814
예
예
817
STTR 의 서비스 큐를 우선순위 낮은 큐로 설정 STTS 의 서비스 큐를 우선순위 높은 큐로 설정
STTR 의 서비스 큐를 우선순위 높은 큐로 설정 STTS 의 서비스 큐를 우선순위 낮은 큐로 설정

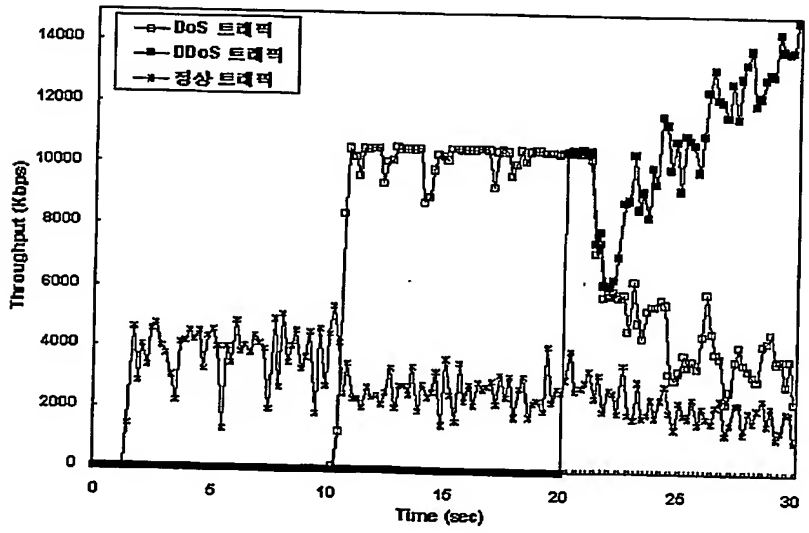
【도 8c】


STT의 부하값에 의한 STT 서비스 큐 결정
819
820
수신된 패킷이 사용한 서비스 큐는 ?
우선순위 낮은큐
우선순위 높은큐
우선순위 높은 큐로 서비스하는 총 패킷 크기 계산
821
822
부하 재계산할 시간 ?
아니오
예
우선순위 높은 큐의 평균 부하 계산
823
우선순위 높은 큐의 부하값에 의한 일부 STT의 서비스큐 재 설정
824
변경된 STT 정보를 큐 정보 테이블에 저장
825

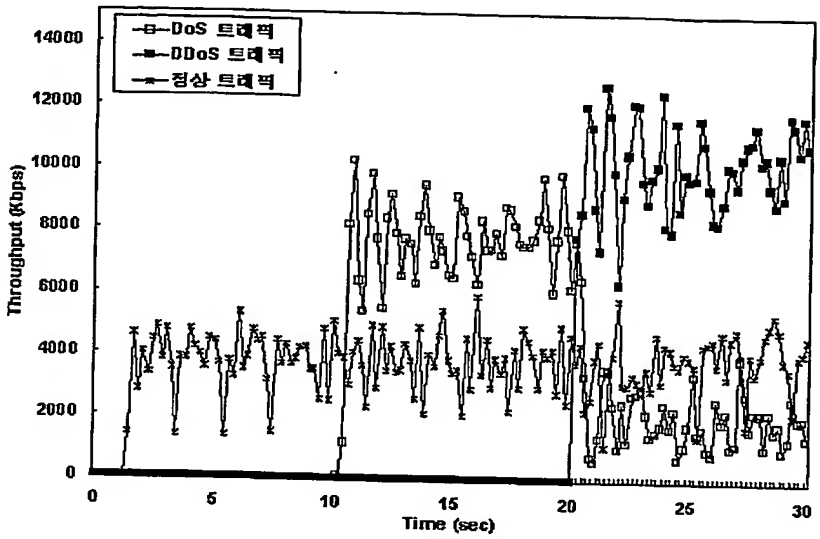
【도 8d】


우선순위 높은 큐의
평균 부하 계산
826
827
우선순위 높은 큐의
부하는 ?
너무 높다(폭주 상태)
너무 낮다(한가 상태)
보통 이다
(안정상태)
828
큐정보 테이블에서
우선순위 높은 큐
사용하는 STT들 중
임의로 하나 선택
829
그 STT 서비스 큐를
우선순위 낮은 큐로 설정
830
큐정보 테이블에서
우선순위 낮은 큐
사용하는 STT들 중
임의로 하나 선택
831
그 STT 서비스 큐를
우선순위 높은 큐로 설정
변경된 STT 정보를
큐 정보 테이블에 저장
832

【도 9a】


DoS 트래픽
DDoS 트래픽
정상 트래픽
Throughput (Kbps)
Time (sec)
0
2000
4000
6000
8000
10000
12000
14000
0
5
10
15
20
25
30

【도 9b】


DoS 트래픽
DDoS 트래픽
정상 트래픽
Throughput (Kbps)
14000
12000
10000
8000
6000
4000
2000
0
0
5
10
15
20
25
30
Time (sec)